ASSESSING THE RISK OF CATASTROPHIC CYBER ATTACK

Lessons from the Electromagnetic Pulse Commission

Research Note

Michael Frankel | James Scouras | Antonio De Simone

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 APR 2015	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Assessing the Risk of Catastrophic Cyber Attack Lessons from the Electromagnetic Pulse Commission	**N00024-13-D-6400**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Michael Frankel James Scouras Antonio De Simone	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
The Johns Hopkins University Applied Physics Laboratory	**NSAD-R-14-116**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
Reflecting on the similarities between cyber and electromagnetic pulse (EMP) attacks, the authors of this Note believe that the approach the EMP Commission used to assess the likelihood and consequences of EMP attacks could provide useful lessons for analysts grappling with the analogous assessment of cyber attacks. To draw such lessons, we need to describe the EMP Commission mandate, describe its approach to addressing that mandate, assess the achievements realized in employing that approach, and understand the extent to which the EMP and cyber attack problems are similar and different. While we draw lessons for cyber analysts, we do not provide recommendations, which should be based on a broader analysis than we have conducted.

15. SUBJECT TERMS
electromagnetic pulse, electric grid, cyber, catastrophic, risk, threat, consequences

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**24**	

ASSESSING THE RISK OF CATASTROPHIC CYBER ATTACK

Lessons from the Electromagnetic Pulse Commission

Michael Frankel

James Scouras

Antonio De Simone

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

This Research Note contains the best opinion of the author(s) at time of issue. It does not necessarily represent the opinion of JHU/APL sponsors.

Distribution Statement A: Approved for public release; distribution is unlimited.

NSAD-R-14-116

Contents

Preface

The increasingly high penetration of cyber systems into essentially all elements of the US economy, coupled with the high rate of apparently unstoppable lower-level cyber intrusions by individuals, groups, and nation-states, has caused great concern that a truly catastrophic cyber attack on the United States may be feasible. Others, however, believe a cyber attack with such severe consequences would be nearly impossible to execute. To date the national debate on this issue can be characterized as a clash of opinions, with neither side well grounded in analysis. Unfortunately, providing a credible analytic basis to shed light on this issue is a daunting challenge.

Reflecting on the similarities between cyber and electromagnetic pulse (EMP) attacks, the authors of this Note believe that the approach the EMP Commission used to assess the likelihood and consequences of EMP attacks could provide useful lessons for analysts grappling with the analogous assessment of cyber attacks. To draw such lessons, we need to describe the EMP Commission mandate, describe its approach to addressing that mandate, assess the achievements realized in employing that approach, and understand the extent to which the EMP and cyber attack problems are similar and different. While we draw lessons for cyber analysts, we do not provide recommendations, which should be based on a broader analysis than we have conducted.

We thank Bilal Ayyub, Christine Fox, Susan Lee, Mark Lewellyn, Thomas Llanso, Thomas Mahnken, Peter Nanos, and Edward Smyth for constructive reviews of earlier drafts of this Research Note.

Very few threats can legitimately raise the specter of catastrophic or existential harm to the nation. A full-scale nuclear attack undoubtedly falls in that category, and the devastating effects of nuclear weapons make the analytic problem straightforward. For other threats—such as electromagnetic pulse (EMP), biological, and cyber attacks—the issue is not as clear-cut. There are limited data and experience with high-end attacks in these domains. However, lack of data and lack of experience do not justify lack of rigor in thinking about attacks with possibly catastrophic consequences.

We believe that studies of any particular catastrophic threat might benefit from the experience of analyzing other such threats. Toward that end, this Note reprises the thought processes and methodology employed by the Commission to Assess the Threat to the United States from Electromagnetic Pulse (the EMP Commission or, simply, the Commission) in the belief that its example may have broader application for assessments of catastrophic threats that share common features of sparsity of data, complex interactivity, and the need for a systems perspective. In particular, we draw analogies to, and lessons for, analyzing potentially catastrophic cyber attacks.

Background

The EMP Commission was established under Title XIV of the 2001 Floyd B. Spence National Defense Authorization Act and charged with assessing:[1]

> (1) The nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next fifteen years;
>
> (2) The vulnerability of United States military and especially civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness;
>
> (3) The capability of the United States to repair and recover from damage inflicted on United States military and civilian systems by an EMP attack; and
>
> (4) The feasibility and cost of hardening select military and civilian systems against EMP attack.

[1] Floyd D. Spence National Defense Authorization for Fiscal Year 2001, Pub. L. No. 106–398, Sec. 1402 [H.R. 5408], 114 Stat. 1654, 1654A-346 (Oct. 30, 2000), www.dod.mil/dodgc/olc/docs/2001NDAA.pdf.

The Commission was also charged with estimating the likelihood that such an attack might occur within the next fifteen years[2] and with recommending "any steps it believes should be taken by the United States to better protect its military and civilian systems from EMP attack."[3] It produced its final reports in 2008 and final testimony to Congress in 2009.[4]

The Commission comprised eminent "formers"—a former national nuclear laboratory director, a retired four-star general, a former presidential science adviser, and a former director of the National Reconnaissance Office—as well as other distinguished scientists from industry and government. Several of the commissioners were experts in the physics of EMP generation and propagation and in the art and science of EMP effects and protection; others were deeply familiar with critical infrastructures, notably energy, telecommunications, and defense. Among them was a common appreciation of the overwhelming scope of their legislative tasking. They were tasked with assessing the likelihood and impact of an event that had never occurred on the military and civilian infrastructures of the entire country, and commissioners at first were uncertain how to proceed.

The first decision the Commission made was essentially to decline to address one of its mandates: assessing the likelihood of an EMP attack in the next fifteen years. Assessing likelihood—which the Commission took to mean estimating a probability with a numerical value between zero and one—would have entailed projections, *inter alia*, of foreign economic, social, and diplomatic developments and how they may affect some future political-military decision calculus by a hostile power. Indeed the Commission would be required to project who would even be considered a hostile power in fifteen years. Would the future political complexion of North Korea's inscrutable leadership incline them toward an EMP attack? Would there even be a North Korea in fifteen years? The Commission did not know how to assign a meaningful probability to such a scenario and did not think anyone else did, either.[5]

---

[2] While this charge is not explicitly articulated in the 2001 National Defense Authorization Act (NDAA), it is explicit in the associated Congressional Record. In addition, the NDAA calls for the secretary of defense to "evaluate the relative likelihood of an EMP attack against the United States compared to other threats involving nuclear weapons."

[3] Pub. L. 106–398.

[4] John S. Foster Jr. et al., "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Executive Report" (July 2004). Also, John S. Foster Jr. et al., "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures" (April 2008), www.empcommission.org/reports.php.

[5] In this regard, the perspective of former Director of the Central Intelligence Agency and Secretary of Defense Robert Gates on the utility of intelligence agency insights resonated strongly: "They really do a very good job of telling you what's going on right now around the world, but forecasting—the truth of the matter is, they're not a lot better than anybody else. And I think policymakers need to understand that." Excerpt from a March 11, 2009, National Public Radio Interview with Scott Siegel, http://centcom.ahp.us.army.mil/index2.php?option=com_content&task=view&id=1404&pop=1&page=0&Itemid=40&lang=en.

Instead, the Commission proceeded on the basis of what it termed a *capabilities-based* threat assessment.[6] Based on an evaluation of current and past technological capability, whether publicly acknowledged or not—and here close coordination with the US intelligence community proved critical—could potential adversaries build or otherwise obtain the necessary technical capabilities to carry out an EMP attack on the United States? What were US vulnerabilities, and what would be the subsequent consequences given that a decision was made to conduct an EMP attack? The Commission's assessment thus addressed what would happen if such weapons were used but did not consider whether an adversary would choose to use such weapons. It thus represented an upper bound on any true threat assessment.

Methodological Issues

The Commission was faced with a number of difficulties in the early phases of analysis. First, there was a relative paucity of hard data. Also, it was faced with the issue of interpreting what failure of one or more components might signify for a system at large. It also worried there were emergent phenomena[7] whose coupling and failure modes might be revealed only with the confluence of the simultaneous failures to be expected in an EMP scenario, at the component and intra- and inter-infrastructural levels. These and other issues left commissioners uncertain at the start as to how to proceed. The Commission eventually converged on a path forward—a series of data gathering and analytic activities that addressed each of these issues. While the subject of its assessment was rather specialized—the effects of EMP on civil and military infrastructures—the sorts of issues previously outlined would seem generic enough that they might apply to a much broader set of societal impact studies, in particular the threat of a massive cyber attack on US infrastructures. With that in mind, we offer the following description of the issues faced and the methodology pursued by the Commission, a summary assessment of the Commission's results, and our own characterization of the Commission's achievements.

Sparse Data

There simply was not an adequate dataset available on the impact of EMP on modern electronic systems that enable and sustain the infrastructures that undergird the

---

[6] *Capabilities-based assessment* is also a term of art in the Department of Defense acquisition community, where it has a quite different meaning. See, for example, National Research Council, *Naval Analytical Capabilities: Improving Capabilities-Based Planning* (Washington, DC: The National Academies Press, 2005), 21–29, www.nap.edu/openbook.php?record_id=11455&page=21.

[7] This is a concept similar to the notion of "hidden interactions" propounded by Charles Perrow in his seminal exposition *Normal Accidents: Living with High-Risk Technologies* (Princeton, NJ: Princeton University Press, 1999), which considered the phenomenon of systems failure from a fresh perspective.

functioning of modern technology-based civil society. While a smattering of individual commercial, industrial, and military components and small systems—televisions, toasters, B-1 bombers—had been tested for their EMP hardness over the years, the rapid evolution of electronic technologies to ever-lower power densities and ever-smaller-scale sizes had rendered much of the already sparse dataset, at best, questionable and, at worst, completely obsolete.

Need for a Systems Perspective

Those data that did exist, or that the Commission was capable of generating itself, were almost entirely related to the failure of small or individual components—a computer chip, a computer, an electronic switch, or an E-6 aircraft. However, what the failure of a component of a system might mean for the overall system response—in which expected failure was often considered in the architectural design—was unclear. What are the implications for the functioning of the US financial system, for example, if data on the failure of a particular circuit board in a telecommunications switch are known, if a transformer in the power grid stops working, or if three transformers and four switches go down? The Commission found such broader questions had not been previously asked and found no credible models to answer them.

Complexity of the Problem

The difficulty in translating component-level data to understanding the full-system response is but one facet of the complexity of the issue. It is certainly difficult enough when the system in question is in reality a system of systems, such as entire national infrastructures like power, telecommunications, banking, food, and transportation. However, the problem of assessing true impact from a national perspective is yet further complicated when the mutual interactions of the different infrastructures themselves need be taken into account. How do failures in one infrastructure affect others? What would failure of communication or transportation links or failure of the power grid to deliver electricity to refrigerators mean for the food infrastructure or the financial infrastructure?

Approaches to Methodological Issues

To address these and many other issues that cropped up, the Commission's efforts fell into three broad categories of focused inquiry.

Data Gathering and Analysis

The Commission reviewed the available data on EMP testing, both publicly accessible and classified work on military systems, and observed failure thresholds for different kinds of

equipment. Concluding early on that the data were both too sparse and too old to form an adequate picture of modern electronic systems with rapidly evolving technologies and architectural changes—especially true for the telecommunications infrastructure, but to a lesser degree for all the infrastructures—the Commission engaged both private contractors and Department of Energy national laboratories to conduct new experiments and generate more modern data. This included, for example, tests conducted on automobiles, cell towers and phone equipment, and power line switches. One of the Commission's more elaborate data gathering and analysis activities involved setting up a model telecommunications network and conducting field tests at a naval facility. The Commission also engaged foreign expertise in the form of work performed by Russian Federation scientists through the auspices of the Russian Academy of Sciences. In the end, the amassed database, while still only a sparse sampling of everything that could have been tested, provided considerable insight on the performance of modern electronics technology to inform EMP vulnerability assessments.

Expert Community Consulting and Analysis

The Commission worked closely with industry-based groups of experts to determine what test data meant for systems operations as a whole. For example, it worked with a special committee of power engineers selected by the North American Electric Reliability Corporation (NERC), a consortium of the major electric grid operators in North America, to understand the implications of failure of single or multiple components for the continued operation of the power grid; with the president's National Security Telecommunications Advisory Committee (NSTAC) for similar insight into the response of the national telecommunications system; and with the Federal Reserve Board for insights into the financial and banking system.

The Commission also consulted experts in the intelligence community. It worked in close consultation with prominent three-letter agencies to obtain insight into existing and prospective technological capabilities of, and technology transfer to, potentially hostile states and to help inform its mandate to perform a threat assessment. Notably, the Commission also engaged in a colloquy with senior military officers from the Russian General Staff who possessed experience with and insight into the threat.

Modeling and Simulation

The Commission engaged in two types of quantitative analytic efforts. One type of effort focused on precise point calculations of physical effects. It calculated the EMP footprints resulting from various detonation scenarios; overlaid them on a network model of the US national electric grid; and, utilizing the failure database, calculated impressed currents and resulting failures of key system components such as extremely high-frequency (EHF) transformers. Armed with the results of such calculations and the insights provided by the

NERC power consultants, the models were then used to calculate the expected outage areas across the United States as point solutions.

Another type of simulation attempted to address the issue of mutually interacting infrastructures. The Commission pursued two parallel efforts with different computational approaches—and ultimately different results. One effort attempted to utilize the developing capabilities for analysis of interdependent infrastructures represented by the National Infrastructure Simulation and Analysis Center (NISAC), then funded by the Department of Energy and currently funded by the Department of Homeland Security. The Commission provided NISAC analysts with an initial condition representing a geographically defined EMP footprint and asked them to calculate the resulting effect on primary civilian infrastructures with full consideration of the infrastructures' mutual interactions, summing up their assessment in terms of an economic impact metric. A similar input was provided to a group of experts at the University of Virginia who applied a classical Leontief input-output model to capture and calculate the economic impact of an EMP attack scenario. The results of the two computational efforts disagreed by almost an order of magnitude, and the cause of this large discrepancy was never resolved. This experience supports the Commission's conclusion that "no currently available modeling and simulation tools exist that can adequately address the consequences of disruptions and failures occurring simultaneously in different critical infrastructures that are dynamically interdependent."[8]

Bottom Lines

In the end, the commissioners were faced with—as the title of the Commission indicates—assessing the threat. However, notwithstanding a robust data gathering and analysis effort, significant uncertainties remained. Also, individual commissioners were not in complete agreement on which bottom line to espouse.

After much deliberation, the Commission coalesced around the following consensus conclusions, which can be found in the final Commission products:[9]

- The high-altitude, nuclear, weapon-generated electromagnetic pulse (EMP) is one of a small number of threats that has the potential to hold our society seriously at risk and might result in defeat of our military forces.
- The damage level could be sufficient to be catastrophic to the nation, and our current vulnerability invites attack.

In our view, what the commissioners are saying, essentially, is that catastrophic damage from an EMP attack *cannot* be ruled out, but, at the same time, such damage cannot be *predicted*.

---

[8] Foster Jr. et al., "Executive Report;" and Foster Jr. et al., "Critical National Infrastructures."

[9] Ibid.

Hence, the emphasis in Commission statements is on what *could* or *might* happen, rather than a more assertive what *would* happen in the event of an EMP attack. Of course, the term *could* covers a lot of territory in probability space, so it is consistent with both low and high likelihoods of catastrophic damage. Although the EMP Commission did not *predict* catastrophic damage, it believed the likelihood that damage would rise to that level was high enough that the nation should act in a comprehensive manner to protect its critical infrastructures.

The EMP Commission did not explicitly define what it meant by "catastrophic" damage, although even a cursory reading of the Commission reports suggests that collapse of the electric grid, either regionally or nationally for an extended period (months to years), qualifies. Another qualifying scenario would be degrading military capabilities to the point that they cannot carry out their intended missions and are in danger of defeat. Note that the Commission did not ever raise the specter of EMP as an "existential" threat to the nation, as has been presumed in a recent Defense Science Board report.[10]

Achievements

In the end, the EMP Commission produced the first large-scale assessment of the impact of a high-altitude EMP event with the potential to degrade or damage the electronic infrastructure supporting the functioning of all facets of modern technology-dependent society. It defined thresholds and identified the potential spectrum of consequences, which ranged from scenarios in which recovery might not be difficult or might not take a long time to more catastrophic scenarios that require much more time for recovery.[11] In short, it bounded, for the first time, the overall physical problem along with some sense of the inherent uncertainty.

Our own perspective is that the EMP Commission made the right decisions by both refusing to assess the likelihood of an EMP attack and emphasizing in its conclusions the potential for a catastrophic attack. Bounding the economic impact of such an event proved to be a more daunting challenge. The Commission developed some reasonable first-order estimates of the cost of restoring the damaged electrical infrastructure—in particular the expected loss and replacement of high-value large transformers and the cost of outfitting

---

[10] Department of Defense Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat" (January 2013), http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[11] Some recently published representations of the Commission's work have mischaracterized its conclusions to assert that it had claimed—with no caveats—that the most catastrophic scenario was the most likely. The Commission did not. Some representations have also included an unfounded claim that the Commission had concluded that two-thirds of the US population would die after an EMP event. The Commission also did not say that.

the system with protective hardware. As described previously, the Commission made two parallel attempts to pursue an economic estimate of the failure of multiple infrastructures, accounting for their interactions, but the scope was limited. This analysis did not encompass the entire US economy, and the different efforts in the end produced inconsistent results. Significant additional work would be needed to address this issue, even if only for a scoping calculation. The assessment also largely neglected many of the "soft science" consequences of an EMP detonation—the psychological, political, and social aftermath.

In summary, we think the Commission provided a solid foundation for further research. Moreover, the lines of attack pursued by the Commission might well hold some lessons for other broad assessment efforts.

Similarities and Differences Between EMP and Cyber Attacks

To assess the relevance of the EMP Commission's experience in assessing the likelihood and consequences of EMP attacks, we first consider the similarities and differences between EMP and cyber attacks.[12] The most obvious similarity is the nature of the target. In both cases, the targets are electronic systems on which the functioning of society depends. Of course, EMP simultaneously threatens all electronic systems in its footprint,[13] while cyber attacks threaten—perhaps simultaneously, perhaps not—only systems that depend on software that can be targeted by cyber weapons. The propagation of effects may be rapid but is highly dependent on the nature of the connected cyber infrastructure under attack. Moreover, cyber weapons need to be tailored to the devices they are targeting. Thus, cyber attacks, even if they are national in scope, will likely be more selective in the systems they target. The effort needed to affect a broad number of systems depends on the number of distinct cyber attack vectors that need to be exploited.

Cyber attacks may proceed by reaching out electronically with encoded signals that instruct a targeted control system to perform a particular unwanted and harmful operation. EMP may function by impressing an unencoded electrical signal that may randomly reset the

---

[12] For an overview of the nexus of EMP, cyber, and geomagnetic threats to infrastructures, see *Electromagnetic Pulse (EMP): Threat to Critical Infrastructure: Hearings Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies*, 113th Cong. (2014) (statement of Dr. Michael J. Frankel).

[13] EMP is a "line-of-sight" phenomenon. That is, if a person on the surface of Earth can "see" a high-altitude nuclear burst, then the location of that person will experience EMP from that burst. A detonation at an altitude of four hundred kilometers, above the surface at Omaha, Nebraska, would thus create EMP across the entire contiguous forty-eight states. Of course, the strength of the pulse falls off as the distance from the burst increases, so locations on the periphery of the EMP footprint would experience fields far weaker than those much closer.

bit state of electronic control systems so that they are unlikely to perform their intended functions. Viewed from this perspective, EMP is a form of "stupid" cyber instruction.

For all practical purposes, neither EMP nor cyber attacks are deterministic, nor are they completely random; thus, their effects on devices are not easily predicted. In an EMP attack, the distribution of initial individual component failures is likely to be distributed in an unpredictable way. All other characteristics being equal, the greater the EMP field strength, the greater the likelihood of damage to a particular component. However, some electronic systems within an EMP footprint exposed to a certain field strength will fail immediately, while similar electronic units in a similar environment will not. Not enough data exist to predict the response of critical systems to EMP.

Similarly, while infrastructures' dependence on cyber systems is pervasive, as are cyber attacks, most of the attacks are nuisances, not the actions of sophisticated adversaries. For predicting the effects on critical systems, nuisance attacks represent mostly noise, not relevant hard data that allow confident predictions. Further, data related to cyber are biased by other factors. Sophisticated adversaries hide their hostile actions. Even when organizations' hostile actions are detected, the organizations are reluctant to share data that show actual or possible compromises to their systems. Thus, the most significant data may in fact be the most difficult to acquire.

There also remains a random component to the failures induced by a cyber attack. Not every targeted system will be in the same state of vulnerability, and the state of any specific system is generally unpredictable. In general, modeling these poorly understood and difficult-to-characterize phenomena associated with both EMP and cyber attacks is far more problematic than modeling completely random or completely deterministic responses.

Predicting the prompt consequences of an EMP attack is largely a problem of physical analysis, while predicting those of cyber attacks must consider rapidly changing software as well as hardware. This rapid change affects both sides of the equation—the attacker must keep pace with the change, and the defender can never be certain protections are adequate.

Ultimately, both EMP and cyber attacks represent threats to systems. Therefore, as with EMP, any relevant analysis must adopt a systems perspective. Some of those systems, particularly those controlling elements of critical infrastructure, certainly can cause physical damage and even death. The ability to cause damage, however, is not the same as a catastrophic threat. It is the cascade and potential multiplication of effects that can be catastrophic. Again, as with EMP, the effects from cyber action need to be analyzed in the context of complex systems of systems at the scale of national infrastructures. The cascade of effects triggered by cyber actions in a complex system represents the same analytic challenge faced by the EMP Commission. These dynamic interdependencies, a feature of the infrastructure under attack, pose one of the greatest challenges to assessing the full range of consequences.

We observe, in summary, that cyber attacks do not clearly pose a more consequential threat than EMP attacks. In addition, the consequences of cyber attacks are not clearly easier to analyze than those of EMP attacks. In fact, the opposite is likely true for both observations. Paraphrasing Churchill's description of the Soviet Union, we might say that trying to assess the consequences of an EMP attack is like trying to solve a riddle wrapped in a mystery inside an enigma.[14] For cyber attacks, the enigma lies within a conundrum.

Lessons for the Cyber Domain

Based on these observations—as well as the EMP Commission experience—we offer the following recommendations for our colleagues working in the cyber domain.

First, because the likelihood of any attack partially depends, in principle, on its anticipated consequences, the likelihood of a cyber attack should be assessed *after* an assessment of its consequences. The EMP Commission refused to directly address likelihood; given the difficulty of assessing cyber consequences, a similar stance may be warranted for assessing the likelihood of cyber attack.

Second, we recommend that cyber analysts provide carefully considered definitions of emotionally laden terms describing consequences, such as *catastrophic* and *existential*. The EMP Commission avoided the term *existential* but did not adequately define *catastrophic*.

Third, the analytic question under consideration needs to be carefully articulated. For example, are analysts trying to establish an upper bound for consequences or a best estimate of the most probable consequences? Is it enough to know, as the EMP Commission determined, that an attack *could* cause catastrophic consequences, or does the analysis need to address whether it *would* do so?

Fourth, the question of consequences must include not only the direct effects of any attack but also potential responses to such an attack. For example, while a cyber attack might not directly cause enough damage to pose an existential threat, is it conceivable that the United States might react to a severe cyber attack in such a manner that the crisis escalates to a nuclear war, which indeed would pose an existential threat to the United States?[15] Although the EMP Commission did not pursue this line of reasoning, doing so may be essential to making the case that a severe cyber attack poses an existential threat.

Fifth, uncertainties need to be identified and analyzed as an inherent part of any cyber consequence assessment. The EMP Commission grappled with uncertainties, rather than

---

[14] Winston Churchill, "The Russian Enigma," BBC Broadcast, London (October 1, 1939).

[15] Martin C. Libicki, *Managing September 12th in Cyberspace: Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies* (Santa Monica, CA: RAND Corporation, 2013). See also Dallas Boyd and James Scouras, "The Dark Matter of Terrorism," *Studies in Conflict and Terrorism* 33 (2010): 1124–1139.

dismiss them. However, it understood that a formal probabilistic analysis of large-scale coupled systems is nontrivial to the point of being infeasible, and that simplistic, probabilistic thinking—relying on independent probabilities and expected values, for example—is inappropriate. The same understanding about the infeasibility of probabilistic risk assessments should inform cyber consequence assessments.

Sixth, EMP effects are difficult to characterize but ultimately are knowable at the device level. The effects are rooted in physics—they can be measured and countered in well-understood and predictable ways. With cyber attacks, even the effects at the device level are uncertain. In many cases, the effects are known, but those cases are not of interest when thinking about nation-state adversaries who rely on difficult-to-acquire technical and operational information and who might be in a position to compromise insiders and operations in ways that are inherently not knowable.

However, for both EMP and cyber attacks, the interaction of device effects with behavior of the larger systems is complex; predicting the effects on infrastructure built of interacting systems is more difficult still. The EMP Commission attempted a modeling and simulation effort that aimed to capture these complex interactions. The Commission's conclusion that no adequate modeling tools exist to describe the further rippling out from systems and infrastructure to economic and social disruptions is a lesson that such consequences cannot be readily predicted. That same lesson applies to other threats, such as cyber threats, that have, at their roots, complexity in execution, uncertainty in effects, and then further complexity in the cascade of consequences that might create catastrophic or existential threats to the nation. The nature of the problem allows for the possibility that such consequences can never be adequately predicted.

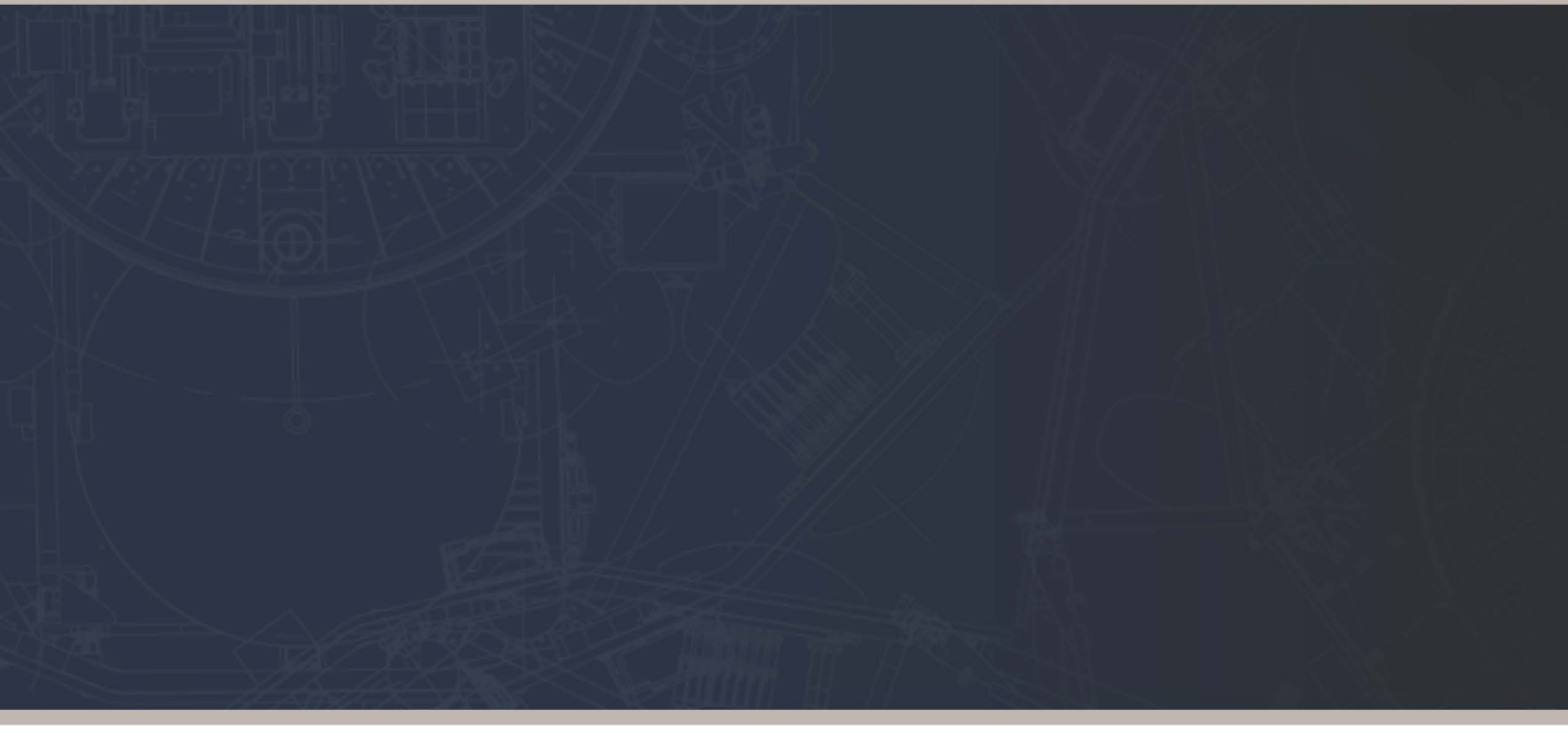
Finally, uncertainty can be pushed aside by focusing on worst-case scenarios. However, large systems inherently can display a wide range of behaviors; worst-case scenarios for complex systems do not necessarily represent realistic cases. The temptation to squelch uncertainty may lead to worst-case thinking at the device level, and then up to the system and infrastructure level, but worst-case thinking in a complex environment does not represent the "plausible worst case" that policy makers need to make decisions.[16] Policy makers cannot act on worst-case threats when the worst case is an extreme that may not be at all plausible in the space of possible outcomes. Strong analysis that embraces, rather than dismisses, complexity is needed to inform decisions at the national level in such cases.

---

[16] For an example of the problem with worst-case thinking in another context, see Jeffrey A. Bader, "Inside the White House during Fukushima: Managing Multiple Crises," *Foreign Affairs*, March 8, 2012, http://www.foreignaffairs.com/articles/137320/jeffrey-a-bader/inside-the-white-house-during-fukushima.

About the Authors

Michael Frankel is a senior scientist at Penn State University's Applied Research Laboratory. James Scouras is a national security studies fellow at the Johns Hopkins University Applied Physics Laboratory. Antonio De Simone is chief scientist of the Johns Hopkins University Applied Physics Laboratory's National Security Analysis Mission Area. Michael Frankel and James Scouras served, respectively, as executive director and staff member of the EMP Commission.



JOHNS HOPKINS
APPLIED PHYSICS LABORATORY